International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-11, April 2014

Reducing Inner Data Stealing Using Bogus Information Attacks in the Cloud Computing

Prof.Mr. Ravikiran Pawar, Mr. Hrishikesh Bhapkar, Mr. Sanket Domal, Mr. Amol Bankar, Mr. Vikrant Dudhale.

Abstract :- Cloud Computing is giving the new approach to use our computers to handle and storing the confidential information. Cloud Computing providing Services like Infrastructure as a Service <IaaS>, Platform as a Service <PaaS> and Software as a Service <SaaS> as well as we have to pay according to our use. The Cloud users can get access over it by the permission of Cloud provider without large investment. As access over Cloud is easily provided by Cloud providers therefore the Security Issues are more in it. The presenting Encryption Strategies are failed to preventing the Inner Data stealing. In this paper we are proposing the completely distinct approach to prevent the Inner data stealing attacks by using offensive decoy technology. When the user is going to access the data we monitoring over it. We are verifying the user by asking him some challenging security questions. Once the user is found that he is unauthorized then we directly applying the decoy information attack over attacker. This will helping us to stop the misuse of the genuine user's data. Using certain functioning we can easily make the evidences against the attacker to stop this malicious activity.

Index Terms: - Cloud Computing, Decoy information, Encryption, malicious, Offensive Decoy Technology.

I. INTRODUCTION

The Cloud Computing really modifies the way to use the data over Cloud. The Cloud user can be outsource his Business, Personal as well as his some confidential data and do processing on that data also.

All this feature of Cloud gets results into the more operational efficiency but at very high level of risk. Among that the Inner Data Staling attack is most serious attack is done on Cloud users. Once the malicious attacker is doing the successful Inner Data Stealing attack on the Cloud then the Service Provider is gets into an important Security matter. As the Inner malicious attacker is doing illegal changes in the cloud and arising new challenges to the Service Provider. So the Cloud Service Provider may not be possible to protect the data. According to the Cloud Security Alliance has giving the top threat priority to this attack [1]. Much more of the Cloud Users are well known about this threat. But still the many of the Cloud Customers are believes that their corresponding Cloud Service Provider handles this threat. There is no transparency and results into the negative quality security issues like control over threat, authentication, authorization etc.

Three years back the Twitter incidence is the suitable example on Inner Data Stealing attack. This incident mainly focused on another security issue in the Cloud Computing Services and resulting into losing the Twitter Customers confidentiality about their data and other files. The leaked files were ex-filtrated to the website TechCrunch [2], [3]. This attack is done on the twitter account of the USA President Barack Obama and the American singer Britney Spears. Their files were also handled illegally [4], [5]. This incidence done by the Inner Data attacker who stolen first-the Twitters admin password and then gain the access over the confidential information, flies of the Twitter Users. This Twitter incidence providing damage to all the Twitter Customers and their corporate data and its privacy across the world.

The attacker was an outsider who stealing the administrators password so to get access like an intrusion insider customer to sniffing the data purposely. As, the Rocha and the Coriea both well explained in detail that how attacker can hack the easy password as a malicious Internal Cloud User. Also they've given some demo of how can attacker take data from the hard disks of the Customers Computer [6].

Many researches are done in the Cloud Computing to update the security mechanisms over threats which arises in the Cloud. More focus of these researches is on the way of preventing the unauthorized access application to the user's information by applying several of the encryption as well as the access control strategies. By applying these all strategies they also has not been fulfill the protections to the data.

According the proof of the Van Dijk and Juels has shown that the completely homomorphic encryption can be a solution to such threats but these are useless mechanism to protect data when it uses alone [7].

Manuscript published on 30 April 2014.
***Correspondence Author(s)
Mr. Hrishikesh Bhapkar, Computer Department, Pune University/ Parvatibai Genba Moze College of Engineering, Pune, India, +918087592357, (e-mail:-hrishikesh.s.bhapkar@gmail.com).
Mr. Sanket Domal, Computer Department, Pune University/ Parvatibai Genba Moze College of Engineering, Pune, India, +919762775047, (e-mail:-sanketdomal@gmail.com).
Prof.Mr.Ravikiran Pawar, , M.Tech Computer Department, Pune University/ Parvatibai Genba Moze College of Engineering, Pune, India, +919881101503, (e-mail:-sunrays@gmail.com).
Mr. Vikrant Dudhale, Computer Department, Pune University/ PGMCO Engineering, Pune, India. +919730801001, (e-mail:-dudhalevikrant@gmail.com).
Mr. Amol Bankar, Computer Department, Pune University/ PGMCO Engineering, Pune, India. +918087848584, (e-mail:-bankaramol92@gmail.com).

Few years ago Stolfo et al. [8] shows a new strategy for the prevention of the insider data theft attacks efficiently. In this paper we are proposing the completely different approach to providing security to the Cloud with the help of decoy information technology. We can call it as Offensive Decoy Technology or Fog Computing. When unauthorized user detection is done after that we propagating the decoy data attack on the malicious internal attacker for the original information security purpose as well as confusing the insider attacker.

The main motive of this proposed system is that we can minimize the damage for the stolen data by the attacker. We provide the protection to our data which is stolen by the attacker by using disinformation attack. Using disinformation attack we are reduce the value of the data or precious information.

In Cloud Computing we are going to achieve by using the User Behavior Profile as well as the Decoy Document. We are proposed both of the strategies to confuse the attacker purposefully to take details of its machines.

In this paper the Section 1 is of Introduction, Section 2 is about the Proposed Security System Mechanism, Section 3 is of Actual Technologies Working and implementation of System, Section 4 is about the Feature Enhancements, Section 5 is finally concludes the paper.

II. PROPOSED SYSTEM SECURITY MECHANISM

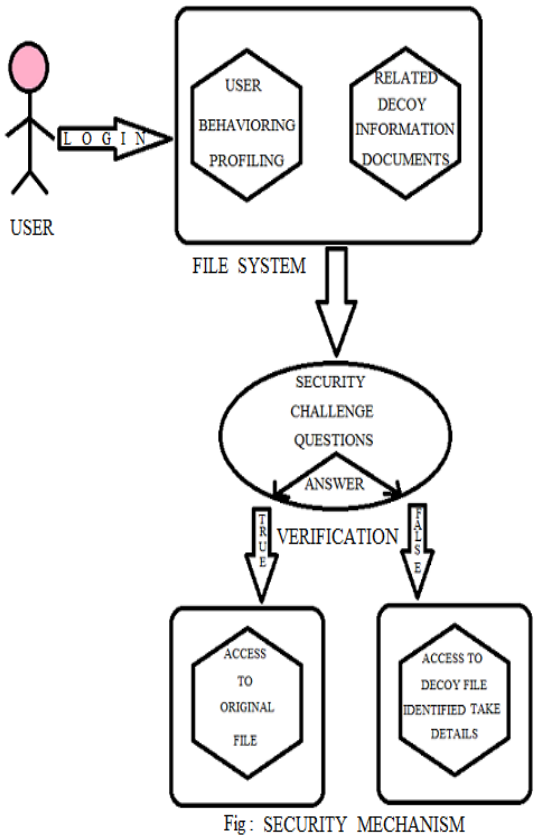

Fig: SECURITY MECHANISM

III. WORKING TECHNOLOGY TERMINOLOGY

In this Section we are mainly seeing the two technology approaches. One is the User Behavior Profiling and second is the Decoy Technology.

By maximize the security here we are make the usage of both of these techniques for the detection of the masquerade attacks done in the cloud. It will helping us for the detection of attacker.

A. *User/Customer Behavior Profiling*

In the cloud the access to the user's documents is done smoothly in the sense of data. So to monitoring the normal usage of the client's account or not. The User Profiling technique is giving the details of the user's that what data is accessed? , how much of data is accessed? , when the data is accessed? Means the general login details of the particular user's actions over the cloud is recorded.

This monitoring over the user is continue for the detection of abnormal access to the information of that customer. Monitoring is implements with the help of behavior based profiling to detect many abnormal usage of data.

Fraud detection system there is the major usage of this profiling technique [9].

B. *Decoy Technology*

Decoy technology is the technology which is providing the decoy information to the unauthorized user or the attacker. Decoy technologies for example honeypot, or the generating the useless data files on the demand of the system to do attack against the attacker. Using this technique the original information gets changed in unexpected format so that the ex-filtering of the document or information is becomes impossible.

Decoy means the relative disinformation, bogus information about the related data documents. This technology is mainly stores some of the decoy data files in the database of the customer as the part of his database. As the decoy files are in same database of the user so that the attacker is gets failed to verify between the actual documents and decoy documents. As the attacker is going to continuing the attack on user's data documents so there is direct linking fog computing sites. So the bogus documents getting receive to the attacker in the much more amount. As the bogus data is gets downloaded by the attacker he gets confused among which data is the actual targeted data. But all the documents are of the bogus types so the original data is gets secured from the malicious insider masquerade attack.

To generate decoy document there is not any specified method or framework. Any data document generation except from the original data document is gets comes under the decoy technology.

C. *Combining The User Behavior Profiling and Decoy Technology*

The combination of the User behavior Profiling and the Decoy Technology is becomes very effective technique to provide the supported stronger evidence of malfeasance. So the combining approach providing more accuracy of the detector's.

The masqueraded attacks are also gets trapped by trap-decoy data. The much more effective Security is provides using this protection mechanism. This is the efficient approach easily implemented to gets stronger security than the existing mechanisms.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Advantages of the Combining Approach:-

(1). Improves the Correctness of the detectors to find out attacker.

(2). Easy and Efficient implementation of the combining technique.

The comparison between searching results and using combined approach experimentally gives the better AUC comparison by user.

The AUC of combined approach is always equal or more than the Searching Profiling result. AUC efficiency of the Combined Approach is does not depend on the number of the users.

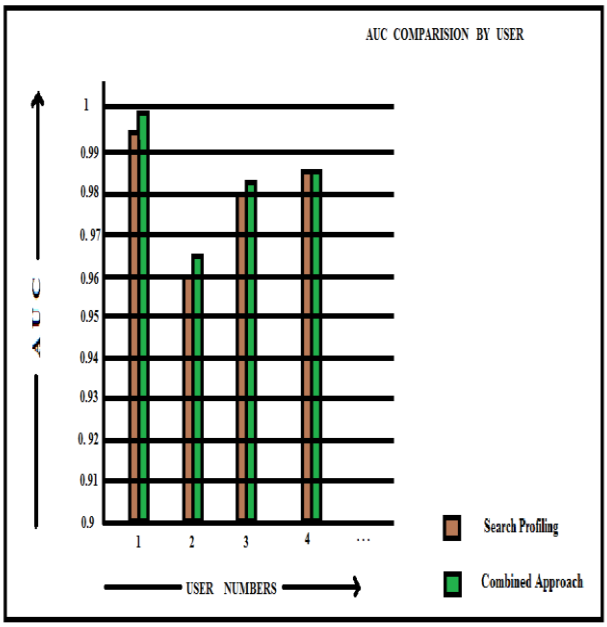

Fig : AUC Comparsion by Number of User

IV. FUTURE ENHANCEMENT

In the future enhancement we have to update the user profiling techniques as much as possible for the detection masquerade actions in cloud.

The decoy documents must be making more attractive so that the attacker easily gets tested.

The identification of attacker process is makes faster than existing process.

V. CONCLUSION

In this paper we stabilize the new approach to secure the cloud on the basis of the concepts of Stolfo et al [8] for security framework. This framework is mainly concentrating on providing the security for preventing internal information theft of the cloud. This prevention is mainly done with the use of combining of two technological approaches. The user behavior profiling technique observes the continuously on user's actions. And the decoy technology is allows to put the decoy documents among the user's data files presented in the database. Decoy data generation dilutes the original data of the user in much more amount of original data. To minimize the inner information stealing by using the combine approach giving us many evidences of the malicious attacker.

REFERENCES

1. Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. [Online]. Available:https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
2. M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July 2009. [Online]. Available: http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-ofconfidentialtwitter-documents/
3. D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted," March 2010. [Online]. Available: http://venturebeat.com/2010/03/24/french-hacker-wholeakedtwitter-documents-to-techcrunch-is-busted/
4. D. Danchev, "ZDNET: french hacker gains access to twitter's admin panel," April 2009. [Online]. Available: http://www.zdnet.com/blog/security/french-hacker-gains-access-totwittersadmin-panel/3292
5. P. Allen, "Obama's Twitter password revealed after french hacker
6. arrested for breaking into U.S. president's account," March 2010.[Online].Available: http://www.dailymail.co.uk/news/article-1260488/Barack-
7. Obamas-Twitter-password-revealed-French-hacker-arrested.html
8. F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," in Proceedings of the First International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments, Hong Kong, ser. DCDV '11, June 2011.
9. M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–8. [Online].
10. Available: http://dl.acm.org/citation.cfm?id=1924931.1924934
11. Salvatore J. Stolfo, Malek Ben Salem and Angelos D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud". IEEE SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOP (SPW) YEAR 2012
12. M. Ben-Salem and S. J. Stolfo, "Modeling user search-behavior for masquerade detection," in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1–20.

AUTHOR PROFILE

Prof. Mr. Ravikiran Pawar,
M.Tech in Computer Science,
Asst. Professor in Parvatibai Genba Moze College of Engineering.
College, Pune
International Publication:-1

Mr. Hrishikesh Bhapkar,
B.E. Computer Department, Pune University/
Parvatibai Genba Moze College of Engineering, Pune.
B.E. Computer (Final Semester.)

Mr. Sanket Domal,
B.E.ComputerDepartment,PuneUniversity/
Parvatibai Genba Moze College of Engineering, Pune.
B.E. Computer (Final Semester.)

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Mr. Amol Bankar,
B.E.ComputerDepartment,PuneUniversity/
Parvatibai Genba Moze College of Engineering,
Pune.
B.E. Computer (Final Semester.)

Mr. Vikrant Dudhale,
B.E.ComputerDepartment,PuneUniversity/
Parvatibai Genba Moze College of Engineering,
Pune.
B.E. Computer (Final Semester.)